PCT WORLD INTELLECTUAL PROPE International Bu

WO 9608756A1

INTERNATIONAL APPLICATION PUBLISHED UNDER

(51) International Patent Classification 6 : G06F 1/00 — A1

(11) International Publication Number: WO 96/08756

(43) International Publication Date: 21 March 1996 (21.03.96)

(21) International Application Number: PCT/GB95/02209

(22) International Filing Date: 18 September 1995 (18.09.95)

(30) Priority Data: 9418709.3 16 September 1994 (16.09.94) GB

(71) Applicant (*for all designated States except US*): CHANTILLEY CORPORATION LIMITED [GB/GB]; 28 Main Street, Mursley, Milton Keynes, Buckinghamshire MK17 0RT (GB).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): HAWTHORNE, William, McMullan [GB/GB]; Kenmare, Bramerton Road, Surlingham, Norwich, Norfolk NR14 7DE (GB).

(74) Agent: GIBSON, S., H.; Urquhart-Dykes & Lord, Three Trinity Court, 21-27 Newport Road, Cardiff CF2 1AA (GB).

(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SECURE COMPUTER NETWORK

(57) Abstract

A secure computer network comprises a plurality of terminals (T1, T2, etc.) connected to a common file server S. Each terminal holds in its memory an encrypted unique variable and unique first and second conjugates for each user authorised to use that terminal. The unique variable is generated, at the time of registration of a user, from master keys stored on a separate disc or other memory medium, the identity number of the terminal, and the identity number of the user to be registered. A password is randomly generated and used to encrypt the unique variable. The first conjugate is a randomly generated message, which is encrypted using the password to generate the second conjugate. In order to log on at a given terminal, the user must enter his password, and the terminal then uses this password as the key to encrypt the first conjugate, and compares it with the stored second conjugate: if the two agree, the terminal is enabled for that person to use. A high level of security is therefore attained.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

Secure Computer Network

This invention relates to computer networks and more particularly to a computer network arranged to provide a high level of security.

It is common in computer networks for individual users to be required to enter their personal passwords in order to gain access to the system. However, present password-based security arrangements are prone to a number of abuses, which undermine the security of the system.

We have now devised a computer network which is arranged to provide a high level of security, and which is not open to degradation of that high level of security.

In accordance with the present invention, there is provided a computer network system which comprises a plurality of individual remote terminals and a central file server, each terminal being arranged to hold, in a memory thereof, an encrypted unique variable and unique first and second conjugates for each user authorised to use that terminal, the second conjugate being a password-encrypted form of the first conjugate.

This system is thus arranged so that in order to log on at a given terminal, the user must enter his password, and the terminal then uses this password as the key to encrypt the first conjugate which is stored at that terminal for that user, and compares that encrypted first conjugate with the stored second conjugate: if the two agree, the terminal is enabled for that person to use.

The system requires each person to register at each terminal which he is intended to use: he cannot use any terminal at which he is not registered.

The system enables each person, once registered, to change his password at will. In order to do this, the system requires the person to log on as described above, then (in response to the user entering the required commands) call up the encrypted unique variable for that user and decrypts that encrypted unique variable, using the user's current password (the encrypted unique variable which is stored being a password

- encryption of the unique variable itself). The system then allows the user to select and enter his own new password, and the terminal then encrypts the user's unique variable with the new password, and creates new first and second conjugates (the second conjugate being a password-encrypted form of the first conjugate, as previously). The terminal now stores, for that user, his new encrypted unique variable and new first and second conjugates, in place of the original ones.

Preferably the system is arranged to create the first conjugate (at initial registration and on change-of-password) on a random basis. Preferably the unique code is generated by the terminal, at initial registration, by a predetermined algorithm and as a function of (a) a master key or set of master keys, (b) a unique identifying number or code for the terminal, and (c) a unique identifying number or code for the particular user to be registered. Preferably the master key (or set of master keys) is entered at the terminal temporarily for each registration procedure, by a security manager. Preferably the master keys are held on a disc or other memory medium normally kept secure by the security manager.

The master key or keys are also held in memory in a secure manner at the central file server. The system is able to transmit data in encrypted form between the file server and terminal and vice versa, in the following manner.

Thus, the user logs on at his terminal, as described above. The system is arranged so that, for the purpose of encrypted transmission, it calls up the user's encrypted unique variable and decrypts this with the user's password. The terminal then randomly generates a session key, and encrypts the session key with the unique variable (preferably however, the terminal also randomly generates an open key and the session key is encrypted with the unique variable and the open key). The encrypted session key (or both encrypted session key and open key) are sent as headers from the terminal to the server, together with the user's identity number. It will be appreciated that because the file server stores the master keys, then it is able to recreate the particular user's unique variable (for the terminal which he is operating) from (a) the master keys, (b) the terminal identity number and (c) the

user's identity number. From this (and from the open key also transmitted as header to the file server), the file server is arranged to determine the random session key.

Communication between the terminal and file server then proceeds with each message being encrypted by the random session key before being sent (whether from the terminal to the server or from the server to the terminal), and decrypted by the random session key at the receiving end. Each terminal may be arranged to change the session key periodically, for example for each new session of use, or at intervals within each session of use.

An embodiment of this invention will now be described by way of example only and with reference to the accompanying drawing, the single figure of which is a schematic diagram of a computer network system in accordance with this invention.

Referring to the drawing, there is shown a typical computer network comprising a plurality of terminals T1,T2 etc connected to a common file server S. In order to register a particular user at a particular terminal, say terminal T1, the security manager carries out the following procedure. Thus, the security manager temporarily loads a disc D at that terminal T1, the disc D holding a plurality of master keys, say 40 keys (typically each key being a number of several digits length). The security manager also enters, at that terminal T1, the identity number of the user being registered. A registration program, held in the terminal or loaded into the terminal from the disc D, then generates a unique variable from (a) the master keys, (b) the identity number of the terminal and (c) the identity number of the user to be registered. An initial password is pseudo randomly generated and given to the user and entered at the terminal T1, and the registration program then encrypts the unique variable using the initial password. Further, the registration program creates first and second conjugates: the first conjugate is a randomly-generated short message in plain, and then the first conjugate is encrypted by the initial password to form the second conjugate; this latter encryption is irreversible in that the first conjugate (or a part thereof) is used to form part of the primitives for the encryption. The registration procedure

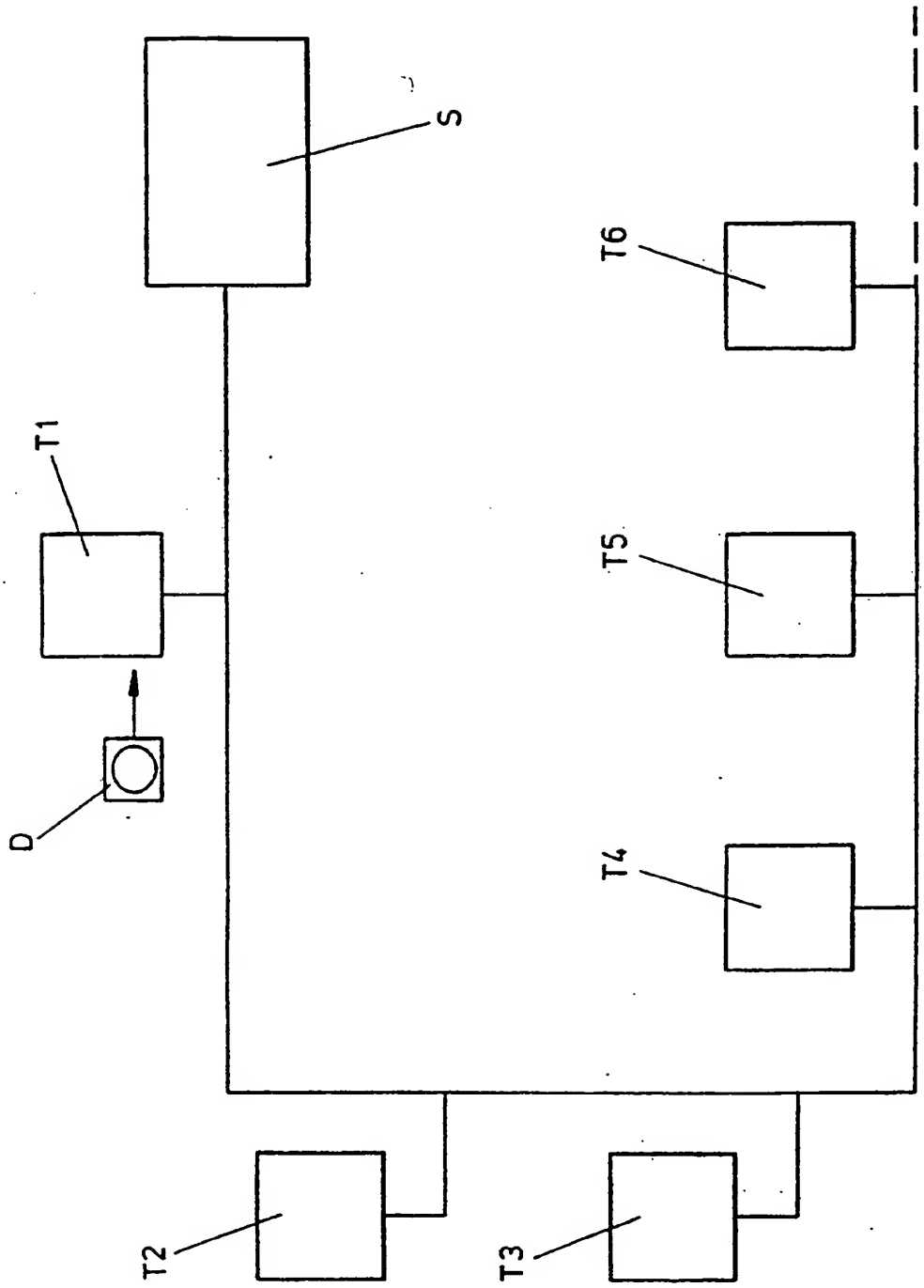
concludes with the terminal T1 storing (a) the encrypted unique variable, (b) the first conjugate and (c) the second conjugate, these being stored at the terminal T1 against the user's name.

In order that the user can now use the network from that terminal T1, he must enter his password for verification. Firstly he enters his name, then his password. Upon entering the password, the terminal T1 (under control of its security program) reads the first conjugate from its memory store, and encrypts this with the password as entered: the result is compared with the second conjugate also held in the memory store; if there is agreement, the entered password is verified and the terminal T1 is enabled for that user to use.

The user, after initial registration, will want to change his initial password to a password known only to himself. In order to do this, firstly he logs on at the terminal T1 for which he is registered, using his initial password in the procedure described above. He then uses the security program to call up the encrypted unique variable, which is held in the terminal's memory against his name, and re-enters his password to decrypt the encrypted unique variable, i.e. giving the unique variable itself. The user then selects his own password, and enters this at the same terminal: the terminal T1 encrypts the unique variable with the new password, and creates new first and second conjugates in the same manner as in initial registration, described above. The terminal T1 then stores, against that user's name, the new encrypted unique variable and the new first and second conjugates, in place of the original ones. In order to log on in future at that terminal, the user must enter his new password for verification, as described previously.

Communication between each terminal T1,T2 etc and the file server S takes place in encrypted manner, as follows. Thus, once a user logs on at a terminal e.g. T1 for which he is registered (in the manner described above), he calls up his encrypted unique variable from the terminal's memory store, and decrypts this by re-entering his password, which recreates the unique variable itself. The terminal's security program now randomly generates an open key and a session key, and encrypts the session key with the unique variable and open key. The

open key and the encrypted session key are sent as headers, together with the user's identity number, to the file server S. The file server S permanently stores the master keys (the same set of master keys which are carried by the security manager's disc D which was loaded temporarily at registration). The file server S is thus able to reconstruct the unique variable for the user at the relevant terminal T1, from (a) the master keys, (b) the terminal number and (c) the user's identity number. The file server S is therefore able, using the reconstructed unique variable and the open key transmitted to it as a header, to determine the random session key from the encrypted session key which it receives from the terminal T1. Communication between the terminal T1 and the file server S then proceeds with each message being encrypted by the random session key before being sent from the terminal T1 to the server S, and the encrypted message being decrypted at the file server S using the random session key reconstructed by the file server S. Communication of messages or data from the file server S to the terminal T1 is similarly encrypted at the server S and decrypted at the terminal T1. The session key can be changed for each new session of use, or it can be changed periodically even within each session of use (e.g. after predetermined intervals of time).


S
T6
T1
T5
D
T4
T2
T3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 95/02209

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP,A,0 421 409 (IBM) 10 April 1991 see abstract; figures 1,4-6,13,14 see page 3, line 35 - page 4, line 13 see page 6, line 18 - page 7, line 5 see page 9, line 55 - page 11, line 19	1,3-7
A	EP,A,0 228 634 (IBM) 15 July 1987 see abstract; figure 1 see page 4, line 51 - page 5, line 4 see page 9, line 19 - line 27	1
A	WO,A,94 04972 (ICL) 3 March 1994	
A	EP,A,0 472 939 (IBM) 4 March 1992	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 January 1996	25. 01. 96

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/GB 95/02209

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0421409	10-04-91	US-A-	5048085	10-09-91
		CA-A-	2026739	07-04-91
		JP-A-	3237551	23-10-91
		US-A-	5148481	15-09-92
EP-A-0228634	15-07-87	US-A-	4805134	14-02-89
		JP-A-	62163155	18-07-87
WO-A-9404972	03-03-94	SE-B-	470366	31-01-94
		EP-A-	0624267	17-11-94
		FI-A-	941891	22-04-94
		SE-A-	9202427	31-01-94
EP-A-0472939	04-03-92	US-A-	5081677	14-01-92
		JP-A-	6019392	28-01-94